

AMENDMENTS TO THE SPECIFICATION

Please amend paragraph [0027] as follows:

--In one embodiment, the method for inserting the infix operators 300 is to copy the applicable operator 202 and insert it between the operands 204 it operates on. In Figure 3, for example, AND is inserted between a and b. Also, OR is inserted between (a AND b) and c. In the embodiment demonstrated with reference to Figure 3, the operands 204 have remained on the line that indicates their position on the prefix Boolean expression tree, and the insertion of the infix operators 300 was done in a manner that preserves these positions. Furthermore, in the embodiment demonstrated with reference to Figure 3, the operands 204 all appear on the right of an invisible line dividing the Boolean expression tree ~~from~~ from the operands 204. This can make the infix operand side of the expression tree easier to read once the infix operators 300 have been inserted.--

Please amend paragraphs [0029]-[0031] as follows:

--In Figure 4, an example of a computer-based system 400 architected in accordance with an embodiment of the present invention is illustrated. System 400 includes agents ~~412~~ 412A, 412B, 412C, one or more managers 414 and one or more consoles 416 (which may include browser-based versions thereof). In some embodiments, agents, managers and/or consoles may be combined in a single platform or distributed in two, three or more platforms (such as in the illustrated example). The use of this multi-tier architecture supports scalability as a computer network or system grows.

Agents ~~412~~ 412A, 412B, 412C are software programs that provide efficient, real-time (or near real-time) local event data capture and filtering from a variety of network security devices

and/or applications. The primary sources of security events are common network elements including firewalls, intrusion detection systems and operating system logs. Agents ~~412~~ 412A, 412B, 412C can collect events from any source that produces event logs or messages and can operate at the native device, at consolidation points within the network, and/or through simple network management protocol (SNMP) traps.

Managers 414 are server-based components that further consolidate; filter and cross-correlate events received from the agents, employing a rules engine 418 and a centralized event database 420. One role of manager 414 is to capture and store all of the real-time and historic event data to construct (via database manager 422) a complete, enterprise-wide picture of security activity. The manager 414 also provides centralized administration, notification (through one or more notifiers 424), and reporting, as well as a knowledge base 428 and case management workflow. The manager 414 may be deployed on any computer hardware platform and one embodiment utilizes a relational database management system such as an OracleTM database to implement the event data store component. Communications between manager 414 and agents ~~412~~ 412A, 412B, 412C may be bi-directional (e.g., to allow manager 414 to transmit commands to the platforms hosting agents ~~412~~ 412A, 412B, 412C) and encrypted.--

Please amend paragraph [0033] as follows:

--In some embodiments, a browser-based version of the console 416 may be used to provide access to security events, knowledge base articles, reports, notifications and cases. That is, the manager 414 may include a web server component accessible via a web browser hosted on a personal or handheld computer (which takes the place of console 416) to provide some or all of the functionality of a console 416. Browser access is particularly useful for security professionals that are away from the consoles 416 and for part-time users. Communication between consoles 416 and manager ~~412~~ 414 is bi-directional and may be encrypted.--

Please amend paragraph [0035] as follows:

--The consoles 416 can similarly be used to author and edit other Boolean expressions, such as rules that control filters. In one embodiment, the rule viewer/editor that creates the user interface to view and edit the rules on the consoles 416 uses a hybrid prefix/infix Boolean expression tree of the variety described with reference to Figure 3. An example rule as displayed by such a display/editor is described with reference to Figure 6. To contrast, [[a]] the example rule is first shown as a pure prefix expression tree in Figure 5.--

Please amend paragraph [0038] as follows:

--The operands 508 are aligned to the left on the right side of the invisible line 510 discussed above. An operand, such as Event Type = correlated, is TRUE or FALSE depending on whether the stated condition is true or false. Such a graphical representation can be very useful and convenient. However, it is difficult to read the rule out loud without first writing it in infix notation. More complicated and lengthy rules become almost impossible to decipher by a human looking at the prefix Boolean expression tree.--

Please amend paragraph [0040] as follows:

--However, to the right of the invisible line 520 is now the infix/prefix hybrid side 604 of the Boolean expression tree. On this side, the operands 508 are still part of the Boolean expression tree. The operands are still on their appropriate vertical lines, such that they remain connected to the prefix Boolean expression tree. However, infix operators 606 have been inserted, so that when read from left-to-right and top-to-bottom (in the manner readers of English and many other languages commonly read), the expression reads as an infix notation expression. In this embodiment, the infix operators ~~602~~ 606 are inserted textually in English/language representation as opposed to symbolically in graphical notation; for example AND instead of &, but in other embodiments graphical equivalents or other languages can be used.--

Please amend paragraph [0045] as follows:

--The present invention is not limited to displaying and editing Boolean expressions. In the foregoing description, the various examples and embodiments were meant to be illustrative of the present invention and not restrictive in terms of ~~heir~~ their scope. Accordingly, the invention should be measured only in terms of the claims, which follow.--